Cybercrime in Nigeria

Current status, Effects and Countermeasures

Temitope O. Ipentan, Asst. Prof.Feon Jaison
MCA (Information Security Management Services)
Jain Deemed-to-be University, Bangalore, India.

Abstract: The alarming evolution of internet over the years has led to security threats for organizations and the people connected to the internet either through mobile or computer. In Nigeria, cybercrimes are carried out daily in various forms such as identity theft, cyber harassment, pornography, piracy and fraudulent electronic mail. The increase in cybercrime in the country has impacted the economy, lives and international reputation. The incessant increase of this crime in the society has become an important issue that should not be overlooked. Therefore, the critical objective of this paper is to discuss the trending cybercrimes in Nigeria, and also the reasons behind the acts which include unemployment and lack of incompetent and strong cybercrime laws. Furthermore, the effects of cybercrime on lives, organizations and country at large, enumerating recommendations and approaches on how to mitigate them.

Keywords: Cybercrime, Nigeria, Scams, Economy

I. INTRODUCTION

Over the years, computers were used by the financial institutions and government research. The act of committing cybercrime was widely limited to those with access and expertise. Today, the technology is predominant and progressively easy to use, ensuring its availability to both the victims and the offenders (Clough, 2010)

The advancement of technology in the society has brought about the use of internet for personal communication and conduct business activities. As these developments have produced great amount of gain for productivity and efficient communication, it has also provided loopholes that can destroy an organization completely. Cybercrime is described as the use of internet or computer to perform any criminal activity (Okeshola and Adeta, 2013).

According to (Lakshmi and Ishwarya, 2015), in 2013, the countries with the highest cyber-attack were United States and South Korea with the value 34.5% and 12.8% respectively. From the last census carried out in 2018, Nigeria has the population of 195 million, a recent statistic revealed that about 92.3 million people have access to the internet. It was also proven that on the penetration of the internet in Africa, 55.5 % are actually Nigerians, hence the higher rate of cybercrime in Nigeria. Cybercrimes are presently performed by people of all ages ranging from the young to the old, but majority by the young.

II. GROWTH OF CYBERCRIME IN NIGERIA

In a research report carried out by Palo Alto Networks, Inc, a US network and enterprise company, the tech Security Company says cyber criminals in Nigeria have evolved from email spam campaigns. They have evolved into more refined techniques that targets large business organizations with malware and has fetched them millions of dollars.

According to the report compiled by the Unit 42 threat research team of the company, they analyzed over 8400 malwares samples originating from the Nigeria scam email from July 2014 to June 2016, indicating roughly 100 actors or group of actors behind these campaigns.

The rate of malware attacks has increased wildly from 100 attacks in July 2014 to a range of 5000 to 8000 monthly and peaking in May 2016 with nearly 19,000 incidents.

According to the tech company the growth of Nigerian actors has increased in size, scope, complexity and capabilities and as a result should be seen formidable threat to business worldwide

These actors have learned how to successfully make use of simple malware tools with precision in order to create great losses ranging from tens of thousands to millions of dollars for the victim organizations. They have also broadened their scope beyond unsuspecting individuals says the report.

Palo Alto identified five of the actors most popular malware tools as Predator Pain, ISR Stealer, Keybase, ISpySoftware and Pony. Each of the tools enable attackers to successfully steal credentials remotely.

Nigerian scammers have moved from flooding random individuals with spam to coordinating surgical spear phishing emails against specific targets. These scammers now carefully craft emails that offer credible propositions to their targets. Most of these emails rely on compromised business emails techniques to make them appear like they originated from a trusted source.

By mapping out the Nigerian social sector, the Unit 42 was able to link the actors to additional malware tools including Nanocore remote access trojan, HawkEye Keylogger, Aegis Crypter and Orway Crypter.

III. EMERGING CYBER TRICKS IN NIGERIA

According to Mayor Mayority, these are the new emerging cyber tricks in Nigeria

Beneficiary of a will scam
An email is sent to the victim from the criminal, claiming the victim is the named beneficiary of an estranged relative's will and stand to win worth of estates and millions

Online Charity
This is another common e-crime carried out by the criminals. They host a fake website for a charity organization, soliciting people for monetary and material contributions. Unsuspecting individuals fall victims to this trick.

Next of kin scam
Collecting money from various banks and transferring fees. By tricking victims to claim billions of dollars belonging to a late relative in a Nigeria bank.

Lottery Scams
This involves deceiving victims into believing they have won an online lottery. Or tricking them to believe they have won a green card lottery.

Computer and internet service time theft
These cyber criminals have developed a way of connecting to the cyber cafe with some Internet service providers (ISP) in a way they don't get detected by the ISP's. which allows the cyber cafes to operate at no cost.

IV. CAUSES OF CYBERCRIME IN NIGERIA

The following are some of the reasons identified to be the causes of cybercrime in Nigeria

Unemployment
This is one of the main concerns in the country, as most of the graduates are unable to gain employment. This is the major reason for cybercrime, according to Labour Force Statics, the unemployment rate is 20.9 million. This has increased the rate in which these graduates get involved in cybercrime in order to survive.

Societal Pressure
The society has influenced so many youths in their decision to engage in cybercrime. Most of the youths are forced to involve in crime in the search for wealth, because of the society standards.

Greed
Greed is another major cause of cybercrime in Nigeria, the youths of nowadays have taken the quest for wealth so far and they are so desperate to make fast money. They are not ready to start little.

Peer Group
Most of the youths involved in cybercrime are influenced by peer pressure. They also want to keep up with their mates and will go to any lengths in order to be influential and remain in the same category with their friends.

Lack of incompetent and strong cybercrime laws
The government also has a big part to play, by equipping the law agencies with new technologies in order to curb cybercrime. Also, strong implementation of laws against cybercrime is needed to be in place.

Lack of infrastructure
In order to carry out proper monitoring and arrest, sophisticated devices are needed by the information and communication Technology center.

Lack of National functional database:
Without a national database tracking down the criminals will be difficult, because there is no way of checking into their past individual records and tracking them

Proliferation of cybercafes
In order to make ends meet, these cybercafes are used as avenues to allow these syndicates to practice their acts through the night services without being monitored

V. EFFECTS OF CYBERCRIMES ON THE COUNTRY

According to the Nigeria Communication Commission (NCC), in 2015, 127 billion naira was the estimated loss to cybercrime in Nigeria, Nigeria currently ranks third globally in cybercrimes behind the United Kingdom and the United states.

Loss of country reputation

The country's reputation for crime has made it unwelcoming to foreign investors and other international governing bodies. Loss of reputation is one of the greatest threats to business and corporate bodies. The lack of trust and confidence in the country protection against cybercrime has hindered profitable transactions between international investors and the country.

Denial of opportunities

The innocent citizens of the country find it challenging getting job opportunities in other countries. Due to the reputation the country has, more than half of Nigerians in foreign countries are seen as fraudsters. People don't want to associate with Nigerians because of the fear of being defrauded by them. Most of the time, these innocent Nigerians are not opportune to use their skills because they are not given the chance to express themselves.

Loss of Information

Information is an important asset to every country including the public and private organizations. Information can be anything ranging from confidential data to non-confidential data. The top data confidential information of the top government official, which gets leaked could cause harm to their work. And if such information is received by a competitor or a perpetrator who has malicious intentions, it could lead to loss of money and loss of reputation to the country or the organization.

Reduced productivity

This is as a result of more concentration being focused on preventing cybercrimes and not showing any productivity. The productivity of a company has been reduced due to the security preventive methods being implemented such as multifactor authentication and other acts that will take time to be carried out thereby affect productivity. The cost spent on software by these organizations to protect their networks such as antivirus and antimalware are exorbitant, because strong security software must be implemented to reduce the possibilities of such attacks.

VI. GLOBAL LEADING PRACTICES

Many developed countries, such as the USA has taken various measures and initiative to train and raise public awareness on cybersecurity, also for law enforcement agencies such

- National cyber security awareness month (under the brand of stop.think.connect)
- National Initiative for Cybersecurity Education (NICE)
- National Cybersecurity Education Council (NCEC)
- Cybersecurity Education and Training Assistance Program (CETAP)
- National Centers of Academic Excellence (CAEs) which provide students valuable technical skills in various disciplines of information assurance

UK has also initiated a national program, Get Safe online whose objective is to raise awareness about cybersecurity to the general public. The government has also published advisory on cybersecurity for the private sectors.

The Australian Government has taken several measures to raise cybersecurity awareness based on age group, such as stay smart online, cybersmart and cybersecurity builder in order to educate and the public about cybersecurity

VII. COUNTERMEASURES AND RECOMMENDATIONS

A nation with a high crime rate cannot develop or grow. This is because crime leaves in its trail a negative social, economic and political consequences (Ribadu, 2004a). Eliminating cybercrime completely cannot be easily achieved but it can be minimized. In order to leverage the impact of cybercrime on the country, it requires the collaborative efforts of the cooperate organizations, individuals and the government. The measures to be taken includes:

Poverty alleviation

Firstly, there is a need to eradicate poverty in the country. Development plan that will boost the economy and provide applicable strategies tackle unemployment and poverty is needed. The major cause of cybercrime is unemployment. The government providing massive employment for the youths will have a long way in minimizing cybercrime. The government should provide and implement programs that the poor will directly benefit from, which can be done by restricting the sources of Nigeria's gross domestic product to importantly include diverse industries that require more labour, such as agriculture and industrialization. Implementing this will provide variation of revenue for the country.

Establishment and enforcement of cyberlaw

Most of the cybercrimes committed go unreported, also most of the victims don't cooperate with the law enforcement when reported. Cooperation of the victims with the law enforcement agencies is needed, whether individuals or organizations, in order to get an effective response. It is important that Nigeria take measures to ensure that its penal and procedural law is adequate and effective enough to meet the challenges posed by the cybercriminals. There must be enforcement by the Government ensuring that the laws are created and strictly adhered to.

Awareness of cybercrimes

Spreading awareness on cybercrime and the prevention techniques to the society is also important, since the cybercriminal invents new ways to attack and target their potential victims. This can be achieved using various media such as bill board, radio, television and the internet so as to ensure faster and maximum reachability using local and national languages. Educating the public on how to defend themselves from being a victim of cybercrime will go a long way in minimizing the amount of cyber-attacks in the country. There is a need for a centralized online cybercrime reporting mechanism; this will provide the victims of cybercrime an easy and convenient avenue to alert the authorities of suspected cybercriminals. This will provide a central database for reference to the law enforcement and regulatory agencies at all level of the country's security.

Introduction of information security in school syllabus

There should be an introduction for the awareness of cybercrime in academics in the early stages of education. Cybercrime awareness should be included into the academic syllabus both for public and private schools. Also, Information security program should be done as a course in the universities. Most of the universities in the country do not provide this course for students to study. Introducing this course in the university syllabus will provide graduates the opportunity of starting firms in information security consultancy, as there are few of them in the country. This also will provide the corporate organizations with enough work power in protecting the network and perimeter security of the organization.

VIII. CONCLUSION

Cybercrime is a threat to the country, which needs to be mitigated or controlled to the minimal level. For Nigeria to go through an economic breakthrough, it must be a crime free nation. But achieving this is clearly impossible, because crime rates increases as technology advancement rises. The attackers also keep up with the technology advancement by coming up with innovative techniques to manipulate their victims. Various ways have been proposed to prevent future occurrence of these crimes, but most importantly the cooperation of the government and the individuals is necessary to minimize them. The government should make the wellbeing of the people a top priority by empowering the youths as they are more involved in these heinous acts, also providing basic amenities for the people will make possible a comfortable life for them, hence reduce the involvement of cybercrime activities and making the country close to being a crime free environment. However, making the country a great nation lies in our hands, most significantly the youth of the nation. The future of country lies on empowering, educating and orientating young people about doing the right thing and it should be the principal importance to the government.

REFERENCES

[1] Adehsina, O.S. (2017). Cybercrime and Poverty in Nigeria. Canadian Social Science**.** 13(4): 19-29. DOI:10.3968/9394

[2] Adomi, E.E., and Stella E. I. (2008). Combating cybercrime in Nigeria. The Electronic Library, 26(5): 716 – 725. http://dx.doi.org/10.1108/02640470810910738

[3] Clough, J. (2010). Principles of cybercrime. Cambridge: Cambridge University Press

[4] Hassan, A.B., Lass, F.D., Makinde, J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN Journal of Science and Technology, 2(7): 626-631

[5] Ibrahim, S. (2016). Causes of socioeconomic cybercrime in Nigeria. International Conference on Cybercrime and Computer Forensic (ICCCF), (pp. 1-9). IEEE. https://doi.org/10.1109/ICCCF.2016.7740439

[6] Lakshmi P., and Ishwarya M. (2015). Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computer and Communication Engineering, 4(3).

[7] Kiru, M.U., and Muhammad, S.I. A Situation Analysis on Cybercrime and its Economic Impact in Nigeria. International Journal of Computer Applications. 169(7): 19-29

[8] Ribadu, N. (2004a), "Problems associated with the enforcement of economic crimes", available at: www.efccnigeria.org (accessed 20 April 2019).

[9] Menon, S., Siew, T.G. (2012). Key challenges in tackling economic and cybercrimes: Creating a multilateral platform for international co-operation. Journal of Money Laundering Control, 15(3):243-256. http://dx.doi.org/10.1108/13685201211238016

[10] Okeshola F.B. and Adeta A.K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State. Nigeria American International Journal of Contemporary Research, 3(9): 98-114

[11] Omodunbi, B.A, Odiase, P. O., Olaniyan, O. M., and Esan. A.O. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology, 1 (1): 37-42